THE STRUCTURE OF NON-ASSOCIATIVE FINITE INVERTIBLE LOOPS (NAFIL)*

RAOUL E. CAWAGAS

ABSTRACT. The NAFIL is a loop in which every element has a unique (two-sided) inverse. NAFIL loops can be classified into two types: *composite* (with at least one non-trivial subsystem) and *non-composite* or *plain* (without any non-trivial subsystem). This paper deals with the structure of these two types of loops. In particular we shall introduce an important class of composite loops called *block products*.

1. Introduction

In a previous paper [2] we introduced the concept of a finite algebra and defined the *non-associative finite invertible loop (NAFIL)*. This is a loop in which every element has a unique (two-sided) inverse and it satisfies all group axioms except the Associative axiom. Because of this, the NAFIL has many structural features in common with the group. However, because the NAFIL is non-associative, it has its own distinctive structure that sets it apart from most algebraic systems.

The study of NAFIL structure is in its early stages and not much information about it is available in the current literature (English). In this paper, we shall begin the study of NAFIL structure by considering the basic properties of NAFIL loops with non-trivial subsystems (**composite**), and those without any non-trivial subsystems (**non-composite** or **plain**).

Before we proceed, let us recall the idea of an *abstract mathematical system* [2, 5]. Such a system essentially consists of: a non-empty set S of distinct elements, at least one binary operation $\star$, an equivalence relation $=$, a set of axioms, as well as a set of definitions and theorems and is usually denoted by $(S, \star)$. The heart of the system is the set of axioms from which all the theorems are derived.

Most algebraic systems like groups, rings, and fields satisfy some or all of the following axioms or postulates:

- A1 - For all $a, b \in S$, $a \star b \in S$. *(Closure axiom)*
- A2 - There exists a unique element $e \in S$, called the *identity*, such that $e \star a = a \star e = a$ for all $a \in S$. *(Identity axiom)*
- A3 - Given an identity element $e \in S$, for every $a \in S$ there exists a unique element $a^{-1} \in S$, called its *inverse*, such that $a \star a^{-1} = a^{-1} \star a = e$. *(Inverse axiom)*
- A4 - For every $a, b \in S$ there exists unique $x, y \in S$ such that $a \star x = b$ and $y \star a = b$. *(Unique Solution axiom)*

- A5 - For every $a, b \in S$, $a \star b = b \star a$. *(Commutative axiom)*
- A6 - For all $a, b, c \in S$, $(a \star b) \star c = a \star (b \star c)$. *(Associative axiom)*

If the set S is of finite order, then $(S, \star)$ is called a *finite system*. In this paper, we shall only consider finite systems.

The simplest algebraic system is the *groupoid*; it is only required to satisfy A1. This is a trivial system and not much can be said about it. A groupoid that also satisfies A4 is called a *quasigroup*; a quasigroup that satisfies A2 is called a *loop*; and a loop that satisfies A3 is called an *invertible loop*. Moreover, an invertible loop that satisfies A6 is called a *group* and one that does not satisfy A6 is called a *NAFIL* (*non-associative finite invertible loop*). In this paper, the word *groupoid* will often be used as a generic term for any system satisfying A1 (like quasigroups, loops, and groups).

2. **Composite NAFIL Loops**

Most mathematical systems contain smaller systems in their structures. Thus, sets can have subsets and groups can have subgroups. Similarly, NAFIL loops can also have subsystems (like loops or groups). To be specific, a subsystem that is a group shall be called a ***subgroup*** while one that is a loop (like the NAFIL) shall be called a ***subloop*** [6]. Otherwise, the word ***subsystem*** shall be used as a generic term for both *subgroup* and *subloop*.

Definition 1. *Let $(S, \star)$ be a loop of order n, and let $\overline{S}$ be a non-empty subset of order m of S. If $(\overline{S}, \star)$ satisfies all axioms satisfied by $(S, \star)$, then it is called a* ***subsystem*** *of $(S, \star)$. Moreover, a subsystem of order m is also called* ***proper*** *if $1 \le m < n$ and* ***improper*** *if $m = n$. If $m = 1$, the proper subsystem is called* ***trivial***; *otherwise it is called* ***non-trivial***.

This definition holds for any groupoid in general. It simply states that if a given system satisfies a set of axioms, then any of its subsystems must also satisfy this set of axioms completely. Thus, a subgroup (or subloop) must satisfy all group (or loop) axioms. Since the group satisfies all NAFIL axioms, then a NAFIL can have a group as a subsystem.

A loop $(\mathcal{L}, \star)$ of order n will be called ***composite*** if it contains at least one non-trivial proper subsystem. A loop is called ***Lagrangian*** if the order m of any of its subsystems is always a divisor (or factor) of n. Otherwise, it is called ***non-Lagrangian.*** Moreover**,** a subloop $(H, \star)$ of a loop $(\mathcal{L}, \star)$ is also said to be ***Lagrange-like*** [6] if the order of H divides the order of $\mathcal{L}$.

Following common practice, we shall also denote the order n of any set S by $|S|$. Moreover, we shall write $\overline{S} \le S$ to mean that $\overline{S}$ is a subsystem of S.

In what follows, we shall introduce and prove a lemma and a number of interesting theorems on subsystems of NAFIL loops. For convenience, we shall often use $\mathcal{L}$ to denote the set of elements $\{\ell_i \mid i = 1, ..., n\}$ of any finite invertible loop, $\overline{\mathcal{L}}$ to denote a subset of $\mathcal{L}$, $1 \equiv \ell_1$ to denote the identity element, and $\ell_i \ell_j$ to denote the product $\ell_i \star \ell_j$, that is, $\ell_i \ell_j \equiv \ell_i \star \ell_j$ if no confusion arises.

Lemma 1. *Let $(\mathcal{L}, \star)$ be an invertible loop of order n and let $\overline{\mathcal{L}}$ be a non-empty subset of order m of $\mathcal{L}$. If $\overline{\mathcal{L}}$ is closed under $\star$ and $T = \{\ell_y \in \mathcal{L} \mid \ell_y \notin \overline{\mathcal{L}}\}$, then: $\ell_x \ell_y$ and $\ell_y \ell_x$ are in T for all $\ell_x \in \overline{\mathcal{L}}$ and all $\ell_y \in T$.*

Proof. Let $\overline{\mathcal{L}} = \{\ell_1, ..., \ell_m\}$ and $T = \{\ell_{m+1}, ..., \ell_n\}$. Since $T = \{\ell_y \in \mathcal{L} \mid \ell_y \notin \overline{\mathcal{L}}\}$, then it follows that $\mathcal{L} = \overline{\mathcal{L}} \cup T$ and $\overline{\mathcal{L}} \cap T = \emptyset$. Hence,

(L1.1)
$$\ell_1, ..., \ell_m, \ell_{m+1}, ..., \ell_n$$

are the n distinct elements of $\mathcal{L}$. Now, let ℓ_x be any element of $\mathcal{L}$ and form the sets:

(L1.2) $\ell_x \overline{\mathcal{L}} = \{\ell_x \ell_1, ..., \ell_x \ell_m\}$ and $\ell_x T = \{\ell_x \ell_{m+1}, ..., \ell_x \ell_n\}$

(L1.3) $\overline{\mathcal{L}} \ell_x = \{\ell_1 \ell_x, ..., \ell_m \ell_x\}$ and $T \ell_x = \{\ell_{m+1} \ell_x, ..., \ell_n \ell_x\}$

Since $(\mathcal{L}, \star)$ is an invertible loop and $\overline{\mathcal{L}} \cap T = \emptyset$, it follows from A1, A4 and Eqs. (L1.2) and (L1.3) that $\ell_x \mathcal{L} = (\ell_x \overline{\mathcal{L}}) \cup (\ell_x T) = \mathcal{L}$ and $\mathcal{L}\ell_x = (\overline{\mathcal{L}}\ell_x) \cup (T\ell_x) = \mathcal{L}$. Next, let $\ell_x \in \overline{\mathcal{L}}$. Since $\overline{\mathcal{L}}$ is closed under $\star$, then $\ell_x \overline{\mathcal{L}} = \overline{\mathcal{L}}\ell_x = \overline{\mathcal{L}}$ and hence it follows that $\ell_x T = T\ell_x = T$. This implies that if $\ell_x \in \overline{\mathcal{L}}$ and $\ell_y \in T$, then $\ell_x \ell_y$, $\ell_y \ell_x \in T$. This completes the proof of the Lemma. ∎

With this Lemma, we can now prove a number of interesting theorems on subsystems of NAFIL loops.

Theorem 1. *Let $(\mathcal{L}, \star)$ be a NAFIL of order n and let $\overline{\mathcal{L}}$ be a non-empty subset of order m of $\mathcal{L}$. If $\star$ is closed on $\overline{\mathcal{L}}$, then $(\overline{\mathcal{L}}, \star)$ is a subsystem of $(\mathcal{L}, \star)$.*

Proof. By hypothesis, $\star$ is closed on $\overline{\mathcal{L}}$. Hence, $(\overline{\mathcal{L}}, \star)$ satisfies A1. By Definition 1 if $(\overline{\mathcal{L}}, \star)$ is a subsystem of $(\mathcal{L}, \star)$, then it must also satisfy A2, A3, and A4. We first prove that $(\overline{\mathcal{L}}, \star)$ satisfies A4. Let $\ell_a, \ell_b \in \overline{\mathcal{L}}$ and let $T = \{\ell_r \in \mathcal{L} \mid \ell_r \notin \overline{\mathcal{L}}\}$. Since ℓ_a, ℓ_b are also elements of $\mathcal{L}$, there exist unique elements ℓ_x and ℓ_y such that $\ell_a \ell_x = \ell_b$ and $\ell_y \ell_a = \ell_b$. Hence, either $\ell_x \in \overline{\mathcal{L}}$ or else $\ell_x \in T$. Suppose $\ell_x \in T$. Then by Lemma 1, $\ell_a \ell_x = \ell_b \in T$. This is a contradiction since $\ell_b \in \overline{\mathcal{L}}$. Therefore, $\ell_x \in \overline{\mathcal{L}}$. Likewise, it follows from Lemma 1 that $\ell_y \in \overline{\mathcal{L}}$. Hence, A4 is satisfied and $(\overline{\mathcal{L}}, \star)$ is at least a quasigroup.

Let ℓ_1 be the identity element of $\mathcal{L}$. Assume that $\ell_1 \in T$ and let $\ell_x \in \overline{\mathcal{L}}$. Then, by Lemma 1, $\ell_x \ell_1 = \ell_x \in T$ which is false since, by hypothesis, $\ell_x \in \overline{\mathcal{L}}$. This implies that $\ell_1 \in \overline{\mathcal{L}}$ and hence A2 is satisfied.

To show that every element in $\overline{\mathcal{L}}$ has an inverse in $\overline{\mathcal{L}}$, let $\ell_a \in \overline{\mathcal{L}}$. Since $\ell_1 \in \overline{\mathcal{L}}$, there exists $\ell_x, \ell_y \in \overline{\mathcal{L}}$ satisfying: $\ell_a \ell_x = \ell_1$ and $\ell_y \ell_a = \ell_1$. By A4, the solution to the these equations is $\ell_x = \ell_y = \ell_a^{-1}$, where ℓ_a^{-1} is the inverse of ℓ_a in $\mathcal{L}$ under $\star$. Hence, ℓ_a^{-1} is in $\overline{\mathcal{L}}$ and A3 is satisfied. Therefore, $(\overline{\mathcal{L}}, \star)$ satisfies A1,A2,A3, and A4 and is thus a subsystem of $(\mathcal{L}, \star)$. This completes the proof of Theorem 1. ∎

Theorem 2. *The order m of any proper subsystem of a composite NAFIL of order n is equal to or less than $n/2$, that is, $m \le n/2$.*

Proof. Let $(\mathcal{L}, \star)$ be a composite NAFIL of order n and let $(\overline{\mathcal{L}}, \star)$ be any proper subsystem of order m. Let $\overline{\mathcal{L}} = \{\ell_1, ..., \ell_m\}$ and $T = \{\ell_{m+1}, ..., \ell_n\}$ such that $T = \{\ell_j \in \mathcal{L} \mid \ell_j \notin \overline{\mathcal{L}}\}$. Then $\ell_1, ..., \ell_m, \ell_{m+1}, ..., \ell_n$ are the n distinct elements of $\mathcal{L}$. Now, let ℓ_j be any element of T. Form the n products:

$$\ell_j \ell_1, ..., \ell_j \ell_m, \ell_j \ell_{m+1}, ..., \ell_j \ell_n$$

By A1 and A4, these n products are the n distinct elements of $\mathcal{L}$ in some order. By Lemma 1, if $\ell_i \in \overline{\mathcal{L}}$ and $\ell_j \in T$, then $\ell_j \ell_i \in T$. Therefore, the m distinct products $\ell_j \ell_1, ..., \ell_j \ell_m$ are all elements of T. This means that T contains at least these m distinct elements. Since T obviously contains $n - m$ distinct elements, then the

following relation must hold: $(n - m) \geq m$. This numerical inequality implies that $m \leq n/2$. Since m also corresponds to the order of $\overline{\mathcal{L}}$, this proves Theorem 2. ∎

This theorem indicates that unlike groups certain NAFIL loops of order n can have a subsystem whose order m is not a divisor of n. Such a system is, therefore, non-Lagrangian. Indeed, there are many known NAFIL loops of this type. Thus, the smallest NAFIL loop $(L_5, *)$ of order $n = 5$ is non-Lagrangian because it has subsystems of order $n = 2$.

$\star$	1	2	3	4	5
1	1	2	3	4	5
2	2	1	5	3	4
3	3	4	1	5	2
4	4	5	2	1	3
5	5	3	4	2	1

Table 1. Cayley table of NAFIL loop $(L_5, *)$ of order n = 5

Remark 1. Lemma 1 and Theorems 1 and 2 hold for loops in general. In fact, they hold even for quasigroups since their proofs essentially depend on A1 and A4.

2.1. **Lagrangian Systems.** Composite systems play a central role in the study of NAFIL structure. One of the most important classes of composite NAFIL loops is the class of **block product systems** [3] that includes *direct products* and *coset products* which are Lagrangian.

The idea of the *block product* is a generalization of the *direct product* concept and is related to groups with a *factor group* (or *group of cosets*) [9] in group theory. This arises from the observation that the Cayley table of a group with a normal subgroup, when its entries are arranged in terms of the cosets of this subgroup, is seen to split up into blocks that is induced by the group operation on the cosets. The entries in each block (called a **coset block**) all belong to a single coset so that each coset can be considered as a single element. These cosets give rise to a partition of the group elements and they form, under certain conditions, a group called the factor group.

The concept of the **coset** [8, 9] in finite group theory is of great importance in the study of associative algebraic structures. The proof of Lagrange's theorem (that the order of a subgroup is a divisor of the order of the group) is based on cosets. This concept, however, does not depend on the associative axiom A6 and it also applies to NAFIL loops and loops in general.

Definition 2. *Let $(H, \star)$ be a subsystem of a composite system $(\mathcal{L}, \star)$ and let $a \in \mathcal{L}$. The subsets $aH = \{a \star \ell \mid \ell \in H\}$ and $Ha = \{\ell \star a \mid \ell \in H\}$ are called the **left** and **right cosets** of H in $(\mathcal{L}, \star)$, respectively. Here, the element a is called a **coset representative**.*

If $K \subseteq \mathcal{L}$ and $K = aH$ (or $K = Ha$), then we also say that K is a left (or right) coset **modulo** H for some $a \in \mathcal{L}$.

Not all composite groups, however, have factor groups (or coset groups). In studying them, the problem posed is to determine the precise conditions under which the elements of such a group can split up into coset blocks with a well-defined operation induced by the group operation on the cosets. A sufficient condition for this is that every left coset is also a right coset. This condition, however, does not hold in general for loops.

2.1.1. **The Block Product**. In this section, we shall present an important system analogous to groups with factor groups that applies to both loops and groups.

Definition 3. *Let $S = \{s_1, \ldots, s_n\}$ be a set of order $n = km$ and let $B = \{B_1, \ldots, B_k\}$ be a partition of S where every $B_i \in B$ is of order m. Let $\times$ and $\diamond$ be quasigroup-type operations on the sets B and S, respectively, such that: If $s_i \in B_p$, $s_j \in B_q$ and $B_p \times B_q = B_r$, then $s_i \diamond s_j = s_h$ for some $s_h \in B_r$. The operations $\times$ and $\diamond$ give rise to two quasigroup-type systems $(B, \times)$ called a **factor system** and $(S, \diamond)$ called a **block product**.*

In this definition the block product $(S, \diamond)$, by analogy, corresponds to the group with a factor group and the factor system $(B, \times)$ corresponds to the factor group (where the cells of the partition B take the place of the cosets and the operation $\times$ is called *cell multiplication*.). However, the roles of the operations $\diamond$ and $\times$ can be viewed in two ways: *(a)* the operation $\times$ is induced by the operation $\diamond$ on B as in the case of factor groups and *(b)* $\diamond$ is induced by $\times$ on S. In either case, the definition does not completely specify these quasigroup operations; it only states a necessary condition that $\diamond$ and $\times$ must satisfy. This incompleteness is what makes the block product concept a useful tool in the construction of composite algebraic systems. It allows us to impose certain requirements on the operations $\diamond$ and $\times$ as well as on the sets S and B to obtain the desired block product.

The Multi$-\Phi$ System

Definition 3 does not explicitly define the block product which can assume several forms. In what follows we shall therefore introduce a particular type of the block product in line with case (a) in which $\times$ is induced by $\diamond$ on B. To do this, we need to present first the concept of the *multi-ϕ system*.

Definition 4. *Let $C = \{c_1, \ldots, c_m\}$ be a set of m elements and let $\Phi = \{\phi_1, \ldots, \phi_g\}$ be a set of g closed binary operations on the set C. The system (C, Φ) is called a **multi-ϕ system** of order $(m; g)$ if it satisfies the following: (I) The system (C, Φ) is at least a quasigroup under every operation $\phi_x \in \Phi$, and (II) Two binary operations $\phi_u, \phi_v \in \Phi$ are **equal**, that is $\phi_u = \phi_v$, if and only if $c_i \phi_u c_j = c_i \phi_v c_j$ for all $c_i, c_j \in C$. If (C, Φ) is of order $(m; 1)$, then it is an ordinary finite system called a **mono-ϕ**.*

The multi-ϕ system (C, Φ) consists of a number of systems (C, ϕ_x) with a common set of elements C. This system is equivalent to what is known as an *indexed algebra* By indexing the operations $\phi_x \in \Phi$, it is possible to compare or distinguish the operations ϕ_x and ϕ_y of any two systems under (C, Φ) by means of their indices x and y.

Because the multi-ϕ system involves operations of various kinds, it becomes necessary to classify systems into types according to the axioms that they are required to satisfy (or not satisfy).

Depending on what axioms a system $(S, \star)$ is required to satisfy, it is usually classified in terms of its *axiom type* as follows:

SYSTEM NAME	AXIOMS SATISFIED	AXIOM TYPE
Groupoid	$A1$	$A[1]$
Quasigroup	$A1, A4$	$A[1,4]$
Loop	$A1, A4, A2$	$A[1,4,2]$
Invertible loop	$A1, A4, A2, A3$	$A[1,4,2,3]$
NAFIL loop	$A1, A4, A2, A3; (\sim A6)$	$A[1,4,2,3](\sim A6)$
Semigroup	$A1, A6$	$A[1,6]$
Monoid	$A1, A6, A2$	$A[1,6,2]$
Group	$A1, A4, A2, A3, A6$	$A[1,4,2,3,6]$
Abelian	Any system satisfying $A5$	$A[5]$

Table 2. Axiom Types of some algebraic systems. (Note: $(\sim A6)$ means *non-associative*.)

A system $(S, *)$ is of *axiom type $A[1,...,x]$* if it satisfies axioms $A1,...,Ax$. This does not imply that these are the only axioms that $(S, *)$ satisfies; it only means that they are specifically required to be satisfied. Thus, an invertible loop is of type $A[1,4,2,3]$ although it may happen that it also satisfies $A5$ and is therefore abelian. If a system is required not to satisfy a given axiom Ax, we shall indicate this by writing $(\sim Ax)$. Thus, the axiom type of the NAFIL is written as $A[1,4,2,3](\sim A6)$.

Henceforth, we shall consider only systems of at least type $A[1,4]$ to be called **quasigroup-type** systems. This includes *quasigroups*, *loops*, *NAFIL loops*, and *groups*. Note that the group and the NAFIL satisfy all *invertible loop* axioms. Because of this, the *group* can also be considered as an *associative invertible loop* while the NAFIL is a *non-associative invertible loop*. Thus, the term *invertible loop* is a generic term for both groups and NAFIL loops.

Since (C, Φ) is a multi-ϕ system, it represents several systems, that is, every $\phi_f \in \Phi$ defines a system (C, ϕ_f) of a given axiom type $A[1,...,x]$. If these systems are all of the same axiom type $A[1,...,x]$, then we simply call (C, Φ) by this common axiom type. Thus, if every $\phi_f \in \Phi$ is a quasigroup operation, then we shall call (C, Φ) a *quasigroup system* for convenience.

2.1.2. **The Block Product as a Generalized Direct Product**. We can now introduce an equivalent definition of the block product given by Definition 3. This is a generalization of the *direct product* [5, 10] in group theory that involves the *multi-ϕ* system.

Definition 5. *Let $(E, *)$ and (C, Φ) be two quasigroup-type systems of orders k and m, respectively, where $\Phi = \{\phi_{pq} \mid p, q = 1, ..., k\}$ is a set of k^2 quasigroup operations, and let $\mathcal{L} = EXC = \{(e_i, c_j) \mid e_i \in E, c_j \in C\}$. The **block product** of $(E, *)$ and (C, Φ) is the system*

$$(\mathcal{L}, \diamond) = (E, *) X (C, \Phi)$$

of order $n = km$, where $\diamond$ is defined by the composition rule:

(D5.1) $$(e_p, c_a) \diamond (e_q, c_b) = (e_p * e_q, \ c_a \phi_{pq} c_b)$$

*and $\phi_{pq} \in \Phi$ for every $e_p, e_q \in E$. If (C, Φ) is a mono-ϕ (when $\phi_{pq} = \phi$ for all p, q), the block product is called a **direct product**. Two elements (e_i, c_x), $(e_j, c_y) \in \mathcal{L}$ are **equal**, that is, $(e_i, c_x) = (e_j, c_y)$, if and only if $e_i = e_j$ and $c_x = c_y$.*

By definition, Φ is a set of k^2 quasigroup operations ϕ_{pq}. The simplest case is that for which $\phi_{pq} = \phi$ for all p, q, that is, if all operations of Φ are equal as in the

simple direct product. Otherwise, each system (C, ϕ_{pq}) under (C, Φ) can assume many forms which determine the properties of the resulting block product $(\mathcal{L}, \diamond)$. The properties of $(\mathcal{L}, \diamond)$ will therefore depend completely on the operation $*$ and the nature of the operations $\phi_{pq} \in \Phi$. By making suitable assumptions about the systems $(E, *)$ and (C, Φ) we can therefore construct composite quasigroup-type structures with desired properties. Because of this, we shall call $(E, *)$ and (C, Φ) the **generating systems** of the block product $(\mathcal{L}, \diamond)$.

The block product of Definition 5 satisfies Definition 3. To show this, we partition the $n = km$ elements of $\mathcal{L}$ into k cells $B_i = \{(e_i, c_u) \mid u = 1, ..., m\}$, each of order m. If this is done all of the m elements $(e_i, c_u) \in B_i$ will have the same e-component e_i, where i has a fixed value. Thus, if $(e_p, c_a) \in B_p$ and $(e_q, c_b) \in B_q$, then by Eq. (D5.1), their product $(e_p * e_q, c_a\phi_{pq}c_b) \in B_r$, where $e_p * e_q = e_r$ is in $(E, *)$. By Definition 3, we can therefore introduce the operation $\times$ of *cell multiplication* and write: $B_p \times B_q = B_r$. This simply means that given any representative element of cell B_p and any representative element of cell B_q, then their product is some element of cell B_r, that is, the operation $\times$ is well defined. The set $B = \{B_i \mid i = 1, ..., k\}$ is therefore closed under $\times$ and hence $(B, \times)$ is at least a groupoid of order k. Clearly, the operations $*$ and $\times$ are seen to be related. This is evident from the fact that it is the operation $*$ of $(E, *)$ that induces the operation $\times$ on B. Here we see, however, that the operations ϕ_{pq} of Φ are not directly related to $\times$.

Let $B_p \times B_q = B_r$. If we form all of the m^2 binary products of the m elements of B_p and the m elements of B_q and arrange them in a table, they will form an $m \times m$ block of entries, denoted by $[B_{pq}] \equiv [B_p \times B_q]$, all of which are elements of B_r. Moreover, since there are exactly k^2 blocks $[B_{pq}]$, then there are exactly k^2 operations $\phi_{pq} \in \Phi$ each of which is defined as a **local operation** over a block $[B_{pq}]$. Henceforth, we shall use this terminology and notation for the operations of the set Φ. Since each $\phi_{pq} \in \Phi$ is a quasigroup-type operation, then each block $[B_{pq}]$ is a Latin square.

The idea of the block product can also be defined for groupoids in general. In this case, the block product of two groupoids will also be a groupoid. Moreover, there is a generalization of the direct product called a **quasidirect product** [6]. This can easily be shown to be a special case of the block product.

2.1.3. **Elementary Properties of Block Products.** Because of the importance of block product systems in the theory of loops and in algebra, we will now determine some of their elementary properties. In what follows, we shall consider block products of the type given in Definition 5.

As defined, the generating systems $(E, *)$ and (C, Φ) of a block product $(\mathcal{L}, \diamond)$ are required only to be at least quasigroups (axiom type *A[1,4]*). This implies that the block product $(\mathcal{L}, \diamond)$ is also a quasigroup as shown by:

Theorem 3. *Let $(E, *)$ and (C, Φ) be quasigroups. Then their block product $(\mathcal{L}, \diamond) = (E, *)\mathsf{X}(C, \Phi)$ is also a quasigroup, and conversely.*

Proof. Let (e_p, c_a), $(e_q, c_b) \in \mathcal{L}$. By Eq. (D5.1) of Definition 5, $(e_p, c_a) \diamond (e_q, c_b) = (e_p * e_q, c_a\phi_{pq}c_b)$. Since $(E, *)$ and (C, Φ) are quasigroups, then $e_p * e_q \in E$, $c_a\phi_{pq}c_b \in C$ and hence $(e_p * e_q, c_a\phi_{pq}c_b) \in \mathcal{L}$. This implies that $(\mathcal{L}, \diamond)$ satisfies *A1* and is at least a groupoid. Now consider the equation

$$(e_p, c_a) \diamond (e_u, c_x) = (e_q, c_b)$$

By Eq. (D5.1), $(e_p, c_a) \diamond (e_u, c_x) = (e_p * e_u, c_a \phi_{pu} c_x)$, where $e_p * e_u \in E$ and $c_a \phi_{pu} c_x \in C$. Since by hypothesis $(E, *)$ and (C, Φ) are quasigroups, then given $e_p, e_q \in E$ and $c_a, c_b \in C$, there exist unique elements $e_u \in E$ and $c_x \in C$ such that $e_p * e_u = e_q$, and $c_a \phi_{pu} c_x = c_b$. Hence, the element $(e_u, c_x) \in \mathcal{L}$ exists and is unique. Similarly, we can show that there exists a unique element $(e_v, c_y) \in \mathcal{L}$ such that:

$$(e_v, c_y) \diamond (e_p, c_a) = (e_q, c_b)$$

Therefore, $(\mathcal{L}, \diamond)$ also satisfies $A4$ from which it follows that it is at least of type $A[1,4]$ and is a quasigroup. Conversely, if $(\mathcal{L}, \diamond)$ is a quasigroup, then $(e_p, c_a) \diamond (e_q, c_b) = (e_p * e_q, c_a \phi_{pq} c_b) \in \mathcal{L}$ and is unique. This implies that $e_p * e_q \in E$ and $c_a \phi_{pq} c_b \in C$ are also unique so that $(E, *)$ and (C, Φ) must also be at least of type $A[1,4]$ and are quasigroups. ∎

The next theorem shows that there is a natural partition of $\mathcal{L}$ that is induced by the operation $*$ of $(E, *)$.

Theorem 4. *Let* $(\mathcal{L}, \diamond) = (E, *) X (C, \Phi)$ *be a block product of order* $n = km$, *where* $(E, *)$ *and* (C, Φ) *are quasigroups,* $E = \{e_1, \ldots, e_k\}$ *and* $C = \{c_1, \ldots, c_m\}$. *Let* $B = \{B_i \mid i = 1, \ldots, k\}$ *where*

(T4.1) $$B_i = \{(e_i, c_u) \in \mathcal{L} \mid u = 1, \ldots, m\}$$

Then (a) B is a partition of $\mathcal{L}$ and (b) the set B forms a quasigroup $(B, \times)$, where $\times$ is cell multiplication.

Proof. (a) It follows from Eq. (T4.1) that any element $(e_i, c_u) \in \mathcal{L}$ is in exactly one subset B_i of $\mathcal{L}$. Hence, $B_i \cap B_j = \emptyset$ if $i \neq j$ and $\bigcup_{i=1}^{k} B_i = \mathcal{L}$ which implies that B is a partition of $\mathcal{L}$. (b) Now, let $(e_i, c_u) \in B_i$ and let $(e_j, c_v) \in B_j$. Then by Eq. (D5.1), $(e_i, c_u) \diamond (e_j, c_v) = (e_h, c_w) \in \mathcal{L}$, where $e_h = e_i * e_j \in E$ and $c_w = c_u \phi_{ij} c_v \in C$. By Theorem 3, $(\mathcal{L}, \diamond)$ is a quasigroup and hence (e_h, c_w) is unique and, by the definition of B_i given by Eq. (T4.1) $(e_h, c_w) \in B_h$, where $B_h \in B$. This means that the operation $\diamond$ of $(\mathcal{L}, \diamond)$ (through the operation $*$ of $(E, *)$) induces on the cells B_x of B a well defined operation $\times$ of *cell multiplication* such that $B_i \times B_j = B_h$ forming a groupoid $(B, \times)$. Next, consider the equation: $(e_p, c_u) \diamond (e_x, c_v) = (e_q, c_w)$, where $(e_p, c_u) \in B_p$, $(e_x, c_v) \in B_x$, and $(e_q, c_w) \in B_q$. Then we have $(e_p, c_u) \diamond (e_x, c_v) = (e_p * e_x, c_u \phi_{px} c_v) = (e_q, c_w)$ which implies that: $e_p * e_x = e_q$ and $c_u \phi_{px} c_v = c_w$. Since $(E, *)$ and (C, Φ) are quasigroups, then $e_x \in E$ and $c_v \in C$ are unique and hence the element $(e_x, c_v) \in B_x$ is also unique. This means that given any two elements $B_p, B_q \in B$, there exists a unique element $B_x \in B$ such that $B_p \times B_x = B_q$. A similar argument also shows that there exists a unique element $B_y \in B$ such that $B_y \times B_p = B_q$. Therefore $(B, \times)$ is also a quasigroup. ∎

Henceforth, we shall refer to the partition $B = \{B_1, \ldots, B_k\}$ of $\mathcal{L}$ defined in Theorem 4 as an ***E-partition*** of $\mathcal{L}$.

Although we have shown that $(B, \times)$ is a quasigroup, it is not necessarily isomorphic to any subsystem of $(\mathcal{L}, \diamond)$. Moreover, $(\mathcal{L}, \diamond)$ does not necessarily have any subsystems isomorphic to $(E, *)$ and (C, Φ). Nevertheless, the operation $\times$ of $(B, \times)$ is clearly induced by the operation $\diamond$ of $(\mathcal{L}, \diamond)$ (through the operation $*$ of $(E, *)$). This indicates that there is a close connection between the structures of $(\mathcal{L}, \diamond)$ and $(B, \times)$.

2.1.4. **Coset Product Loops.** Let us now consider an important form of the block product, called the **coset product** [3], that is closely related to the idea of the group with a coset group (or quotient group) in finite group theory.

This is the interesting case when the block product $(\mathcal{L}, \diamond) = (E, *) \mathsf{X} (C, \Phi)$ is a loop (like a NAFIL or a group) with a normal subloop $(B_1, \diamond)$, where $B_1 \subset B$, and the system $(B, \times)$ is also a loop such that every $B_i \in B$ is a coset of B_1. For this particular case, we shall therefore call B the *E-partition of* $\mathcal{L}$ (mod B_1). This must be distinguished from other E-partitions of $\mathcal{L}$ in which $(B_1, \diamond) \in B$ is not a loop.

In constructing a coset product, it is important to be specific about the nature of the generating systems $(E, *)$ and (C, Φ). By Definition 4, the multi-ϕ (C, Φ) represents several systems with a common set of elements C. Therefore, each of these systems (C, ϕ_{pq}) under (C, Φ) must be clearly defined. In particular, if (C, ϕ_{pq}) is a loop, its identity element must be identified. This leads us to classify multi-ϕ loops (C, Φ) into two major types: **Type A** when (C, Φ) has a common identity element for all $\phi_{pq} \in \Phi$ and **Type B** otherwise.

To fix the meaning of the coset product, we need to introduce a number of important concepts.

Definition 6. *Let $(\mathcal{L}, \diamond)$ be a loop of order $n = km$ with a subloop $(B_1, \diamond)$ of order m. Then $(B_1, \diamond)$ is called **normal** if the set $B = \{B_i \mid i = 1, ..., k\}$ of cosets of B_1 forms a loop $(B, \times)$ of order k called a **factor system**.*

This definition implies that the left and right cosets of B_1 are always equal and that B is an *E-partition of* $\mathcal{L}$ (mod B_1). For a group (which is associative), this is a sufficient condition for a subgroup to be normal. For a non-associative loop (like the NAFIL), however, a subsystem whose cosets form a partition of $\mathcal{L}$ is not necessarily normal. By Definition 6 the set B of cosets of B_1 must form a factor system $(B, \times)$ for $(B_1, \diamond)$ to be normal. If $(B_1, \diamond)$ is normal in $(\mathcal{L}, \diamond)$, we can formally write: $(\mathcal{L}, \diamond) / (B_1, \diamond) = (B, \times)$.

$\diamond$	ℓ_1	ℓ_2	ℓ_3	ℓ_4	ℓ_5	ℓ_6	ℓ_7	ℓ_8
ℓ_1	ℓ_1	ℓ_2	ℓ_3	ℓ_4	ℓ_5	ℓ_6	ℓ_7	ℓ_8
ℓ_2	ℓ_2	ℓ_3	ℓ_4	ℓ_1	ℓ_6	ℓ_7	ℓ_8	ℓ_5
ℓ_3	ℓ_3	ℓ_4	ℓ_1	ℓ_2	ℓ_7	ℓ_8	ℓ_5	ℓ_6
ℓ_4	ℓ_4	ℓ_1	ℓ_2	ℓ_3	ℓ_8	ℓ_5	ℓ_6	ℓ_7
ℓ_5	ℓ_5	ℓ_6	ℓ_7	ℓ_8	ℓ_1	ℓ_2	ℓ_3	ℓ_4
ℓ_6	ℓ_6	ℓ_5	ℓ_8	ℓ_7	ℓ_2	ℓ_1	ℓ_4	ℓ_3
ℓ_7	ℓ_7	ℓ_8	ℓ_5	ℓ_6	ℓ_3	ℓ_4	ℓ_1	ℓ_2
ℓ_8	ℓ_8	ℓ_7	ℓ_6	ℓ_5	ℓ_4	ℓ_3	ℓ_2	ℓ_1

3(A).$(\{\ell_1, \ell_2, \ell_3, \ell_4\}, \diamond)$ is normal

$\diamond$	ℓ_1	ℓ_7	ℓ_2	ℓ_8	ℓ_3	ℓ_5	ℓ_4	ℓ_6
ℓ_1	ℓ_1	ℓ_7	ℓ_2	ℓ_8	ℓ_3	ℓ_5	ℓ_4	ℓ_6
ℓ_7	ℓ_7	ℓ_1	ℓ_8	ℓ_2	ℓ_5	ℓ_3	ℓ_6	ℓ_4
ℓ_2	ℓ_2	ℓ_8	ℓ_3	ℓ_5	ℓ_4	ℓ_6	ℓ_1	ℓ_7
ℓ_8	ℓ_8	ℓ_2	ℓ_7	ℓ_1	ℓ_6	ℓ_4	ℓ_5	ℓ_3
ℓ_3	ℓ_3	ℓ_5	ℓ_4	ℓ_6	ℓ_1	ℓ_7	ℓ_2	ℓ_8
ℓ_5	ℓ_5	ℓ_3	ℓ_6	ℓ_4	ℓ_7	ℓ_1	ℓ_8	ℓ_2
ℓ_4	ℓ_4	ℓ_6	ℓ_1	ℓ_7	ℓ_2	ℓ_8	ℓ_3	ℓ_5
ℓ_6	ℓ_6	ℓ_4	ℓ_5	ℓ_3	ℓ_8	ℓ_2	ℓ_7	ℓ_1

3(B). $(\{\ell_1, \ell_7\}, \diamond)$ is not normal

Table 3. Cayley tables of a NAFIL loop $(\mathcal{L}, \diamond)$ of Order n = 8.

To understand this concept of normality, consider the non-abelian NAFIL $(\mathcal{L}, \diamond)$ of order $n = 8$ whose Cayley table is shown in two forms in Table 3. Analysis (using the software FINITAS [4]) shows that $(\mathcal{L}, \diamond)$ has 8 non-trivial subsystems all of which are groups: 3 of order 4 (1 isomorphic to C_4 and 2 are isomorphic to K_4) and 5 of order 2 (isomorphic to C_2). Out of these 8 subgroups, 6 have cosets that form partitions of $\mathcal{L}$. In particular, the 3 subgroups of order 4 are all **normal**, that is, their cosets form partitions B of $\mathcal{L}$ such that $(B, \times)$ is a factor

system of $(\mathcal{L}, \diamond)$. Table 3(A) shows $(\mathcal{L}, \diamond)$ arranged in terms of the normal subsystem $(\{\ell_1, \ell_2, \ell_3, \ell_4\}, \diamond)$ of order 4 while Table 3(B) shows $(\mathcal{L}, \diamond)$ arranged in terms of the subsystem $(\{\ell_1, \ell_7\}, \diamond)$ of order 2 which is not normal.

The three subgroups of order 2 whose cosets also form partitions, however, are not all normal. For instance, the subgroup $(\mathcal{B}_1, \diamond) \cong C_2$, where $\mathcal{B}_1 = \{\ell_1, \ell_7\}$, has the following cosets: $\mathcal{B}_1 = \{\ell_1, \ell_7\}$, $\mathcal{B}_2 = \{\ell_2, \ell_8\}$, $\mathcal{B}_3 = \{\ell_3, \ell_5\}$, $\mathcal{B}_4 = \{\ell_4, \ell_6\}$ that form the partition $\mathcal{B} = \{\mathcal{B}_1, \mathcal{B}_2, \mathcal{B}_3, \mathcal{B}_4\}$ of $\mathcal{L}$. However, this set $\mathcal{B}$ of cosets of $\mathcal{B}_1$ is not closed under cell multiplication $\times$. To verify this, consider the cell $\mathcal{B}_2 = \{\ell_2, \ell_8\}$. If $\mathcal{B}$ is closed under $\times$, then the product of any two elements of $\mathcal{B}_2$ must belong to just one cell $\mathcal{B}_x \in \mathcal{B}$. But $\ell_2 \diamond \ell_8 = \ell_5 \in \mathcal{B}_3$ and $\ell_8 \diamond \ell_2 = \ell_7 \in \mathcal{B}_1$. Hence, $\mathcal{B}_2 \times \mathcal{B}_2$ is not defined and therefore $\mathcal{B}$ is not closed under $\times$. This means that $(\mathcal{B}_1, \diamond)$ is not normal and the set $\mathcal{B}$ of cosets of $\mathcal{B}_1$ is not an E-partition of $\mathcal{L}$ (mod $\mathcal{B}_1$).

In the study of coset products we will have occasion to consider multi-ϕ systems (C, Φ) containing quasigroups in which the existence of a unique identity or unique inverses are not assumed. In such systems, we will consider weaker forms of $A2$ and $A3$ involving two kinds of identity elements and two kinds of inverse elements [6, 8].

Definition 7. *Let $(\mathcal{L}, \diamond)$ be a quasigroup. Then $1^\lambda \in \mathcal{L}$ is called a **left identity** if and only if $1^\lambda \star \ell = \ell$ and $1^\rho \in \mathcal{L}$ is called a **right identity** if and only if $\ell \star 1^\rho = \ell$ for all $\ell \in \mathcal{L}$.*

Definition 8. *Let $(\mathcal{L}, \star)$ be a loop whose identity element is $\ell_1 \equiv 1$ and let $\ell \in \mathcal{L}$. Then $\ell^{-\lambda}$ and $\ell^{-\rho}$ are called the **left inverse** and **right inverse** of ℓ, respectively, if and only if $\ell^{-\lambda} \star \ell = 1$ and $\ell \star \ell^{-\rho} = 1$. If $\ell^{-\lambda} = \ell^{-\rho} \equiv \ell^{-1}$ such that $\ell^{-1} \star \ell = \ell \star \ell^{-1} = 1$, then ℓ^{-1} is called the **two-sided inverse** or simply the **inverse** of ℓ.*

Theorem 5. *Let $(\mathcal{L}, \diamond)$ be a block product of order $n = km$ whose generating system $(E, *)$ is a loop whose identity is e_1 and (C, Φ) is a multi-ϕ system such that every (C, ϕ_{ij}) has a common identity element c_1. Then: **(a)** $(\mathcal{L}, \diamond)$ is also a loop whose identity element is (e_1, c_1). **(b)** If $B = \{B_1, \ldots, B_k\}$ is the E-partition of $\mathcal{L}$, then $(B_1, \diamond)$ is a subsystem of $(\mathcal{L}, \diamond)$. **(c)** The system $(B, \times)$, where $\times$ is cell multiplication, is a loop isomorphic to $(E, *)$ and is a factor system of $(\mathcal{L}, \diamond)$. Hence, $(B_1, \diamond)$ is normal.*

Proof. **(a)** By Theorem 3, $(\mathcal{L}, \diamond)$ is at least a quasigroup. Let $E = \{e_1, ..., e_m\}$ and $C = \{c_1, ..., c_k\}$. Since $(E, *)$ is a loop, then it has a unique identity element, say e_1. By hypothesis (C, Φ) is a multi-ϕ system such that every (C, ϕ_{ij}) has a common identity element c_1. Now, let $(e_1, c_1), (e_i, c_j) \in \mathcal{L}$ and form the products:

$$(e_i, c_j) \diamond (e_1, c_1) = (e_i * e_1, c_j \phi_{i1} c_1) = (e_i, c_j)$$
$$(e_1, c_1) \diamond (e_i, c_j) = (e_1 * e_i, c_1 \phi_{1j} c_j) = (e_i, c_j)$$

Therefore, we find that

$$(e_1, c_1) \diamond (e_i, c_j) = (e_i, c_j) \diamond (e_1, c_1) = (e_i, c_j)$$

which implies that the element $(e_1, c_1) \in \mathcal{L}$ is a unique identity element under $\diamond$. Hence, the quasigroup $(\mathcal{L}, \diamond)$ also satisfies $A2$ and is therefore a loop (type $A[1,4,2]$).

(b) If $B = \{B_1, ..., B_k\}$ is an E-partition of $\mathcal{L}$, then $B_1 = \{(e_1, c_u) \in \mathcal{L} \mid u = 1, \ldots, m\}$ and thus the identity element $(e_1, c_1) \in B_1$. Now let $(e_1, c_u), (e_1, c_v) \in B_1$.

Then $(e_1, c_u) \diamond (e_1, c_v) = (e_1 * e_1, c_u \phi_{11} c_v) = (e_1, c_w)$, where $c_w = c_u \phi_{11} c_v \in C$. Clearly, $(e_1, c_w) \in B_1$ and therefore B_1 is closed under $\diamond$. By Theorem 1, this implies that $(B_1, \diamond)$ is a subsystem of $(\mathcal{L}, \diamond)$ and is thus also a loop.

(**c**) By Theorem 4, since B is an *E-partition* of $\mathcal{L}$, then $(B, \times)$ is at least a quasigroup of order k, where $\times$ is cell multiplication. Hence, if $B_i, B_j \in B$, then we can write: $B_i \times B_j = B_h$, where $B_h \in B$. In (a) we have shown that $(\mathcal{L}, \diamond)$ is a loop whose identity is (e_1, c_1) and that if $(e_1, c_u), (e_1, c_v) \in B_1$, then their product $(e_1, c_u) \diamond (e_1, c_v) \in B_1$ and we can write: $B_1 \times B_1 = B_1$. Now, let $(e_1, c_u) \in B_1$ and $(e_x, c_v) \in B_x$. Form the products:

$$(e_1, c_u) \diamond (e_x, c_v) = (e_1 * e_x, c_v \phi_{1x} c_u) = (e_x, c_v \phi_{1x} c_u) \in B_x$$
$$(e_x, c_v) \diamond (e_1, c_u) = (e_x * e_1, c_v \phi_{x1} c_u) = (e_x, c_v \phi_{x1} c_u) \in B_x$$

This means that we can write: $B_1 \times B_x = B_x \times B_1 = B_x$, which implies that B_1 is an identity element under $\times$. Hence, the quasigroup $(B, \times)$ satisfies A2 and is therefore a loop. To prove that $(B_1, \diamond)$ is normal, we first show that every $B_i \in B$ is a left/right coset of B_1. Let $(e_x, c_v) \in \mathcal{L}$ and $(e_1, c_u) \in B_1$. By Theorem 4, $B_1 = \{(e_1, c_u) \in \mathcal{L} \mid u = 1, \ldots, m\}$ so that the left and right cosets of B_1 are:

$$(e_x, c_v) \diamond B_1 = \{(e_x * e_1, c_v \phi_{x1} c_u) \mid x = 1, \ldots, k, \ u, v = 1, \cdots, m\}$$
$$B_1 \diamond (e_x, c_v) = \{(e_1 * e_x, c_u \phi_{1x} c_v) \mid x = 1, \ldots, k, \ u, v = 1, \ldots, m\}$$

Since e_1 is the identity of E, then $e_1 * e_x = e_x * e_1 = e_x$ and since C is closed under every $\phi_{pq} \in \Phi$, then we find that $(e_x, c_v) \diamond B_1 = B_1 \diamond (e_x, c_v) = B_x \in B$. Therefore, every left coset of B_1 is also a right coset and that they form the *E-partition B of* $\mathcal{L}$ (mod B_1). Clearly, the correspondence

$$e_i \leftrightarrow B_i, \ e_j \leftrightarrow B_j, \ e_i * e_j \leftrightarrow B_i \times B_j$$

defines an isomorphism between $(E, *)$ and $(B, \times)$. Since, by hypothesis, $(E, *)$ is a loop, this shows again that $(B, \times)$ is a loop under cell multiplication $\times$. Finally, since $(B, \times)$ is a loop, then it is a factor system of $(\mathcal{L}, \diamond)$. Therefore $(B_1, \diamond)$ is normal. ∎

In Theorem 5, we showed that if the block product $(\mathcal{L}, \diamond) = (E, *) \mathsf{X} (C, \Phi)$ is a loop and $B = \{B_1, \ldots, B_k\}$ is the E-partition of $\mathcal{L}$ (mod B_1), then $(B_1, \diamond)$ is a normal subsystem of $(\mathcal{L}, \diamond)$. For such a system, each cell $B_i \in B$ is a coset of B_1 so that we can call the operation $\times$ of cell multiplication in $(B, \times)$ as *coset cell multiplication* and $(\mathcal{L}, \diamond) = (E, *) \mathsf{X} (C, \Phi)$ as a **coset product**.

Definition 9. *A block product* $(\mathcal{L}, \diamond) = (E, *) \mathsf{X} (C, \Phi)$ *is called a **coset product** if and only if it is a loop with a normal subsystem* $(B_1, \diamond)$*, where the set* $B = \{B_1, \ldots, B_k\}$ *of cosets of* B_1 *is an E-partition of* $\mathcal{L}$ (mod B_1).

Note that Theorem 5 holds for loops in general provided that (C, Φ) has a common identity element (Type A). The system $(B, \times)$ is the loop of cosets of B_1 under the induced operation $\times$ and is a factor system of $(\mathcal{L}, \diamond)$ modulo B_1. If (C, Φ) has no common identity element (Type B), the resulting coset product $(\mathcal{L}, \diamond)$ will still be a loop. This will be the case if (C, Φ) is such that every (C, ϕ_{ij}) has an element c_1 that is at least a right identity if $j = 1$ and a left identity if $i = 1$.

We also note that $(B, \times)$ is isomorphic to $(E, *)$. But $(\mathcal{L}, \diamond)$ does not necessarily have any normal subsystem isomorphic to $(E, *)$ and hence to $(B, \times)$. If $(\mathcal{L}, \diamond)$ has

such a normal subsystem isomorphic to $(E, *)$, we shall call $(\mathcal{L}, \diamond)$ an **extension** [6] of $(E, *)$ by (C, Φ).

Coset Products with Type A and B (C, Φ) Loops

The next theorem deals with coset products that are *invertible loops* (like NAFIL loops and groups). This theorem considers the case when the loops (C, ϕ_{pq}) under (C, Φ) have a common identity element (Type A).

Theorem 6. *If $(E, *)$ and (C, Φ) are invertible loops, where (C, Φ) has a common identity element for all $\phi_{pq} \in \Phi$ such that $\phi_{pq} = \phi_{qp}$, then their coset product $(\mathcal{L}, \diamond) = (E, *)X(C, \Phi)$ is also an invertible loop.*

Proof. By Theorem 5, $(\mathcal{L}, \diamond)$ is a loop if its generating systems $(E, *)$ and (C, Φ) are loops. Therefore, it remains to show that if $(E, *)$ and (C, Φ) are invertible loops, where (C, Φ) has a common identity, then so is $(\mathcal{L}, \diamond)$. By definition, a loop is invertible if every element has a unique inverse. Since $(E, *)$ and (C, Φ) are invertible, then every element in these loops has a unique inverse. Let (e_p, c_i) and $(e_q, c_j) \in \mathcal{L}$ such that $e_p * e_q = e_q * e_p = e_1$ and $c_i \phi_{pq} c_j = c_j \phi_{qp} c_i = c_1$, where $\phi_{pq} = \phi_{qp}$, and e_1 and c_1 are the identity elements of E and C, respectively. Form the products:

$$(e_p, c_i) \diamond (e_q, c_j) = (e_p * e_q, \, c_i \phi_{pq} c_j) = (e_1, c_1)$$
$$(e_q, c_j) \diamond (e_p, c_i) = (e_q * e_p, \, c_j \phi_{qp} c_i) = (e_1, c_1)$$

where (e_1, c_1) is the identity element of $(\mathcal{L}, \diamond)$. Thus we find that

$$(e_p, c_i) \diamond (e_q, c_j) = (e_q, c_j) \diamond (e_p, c_i) = (e_1, c_1)$$

which implies that (e_p, c_i) and (e_q, c_j) are unique inverses in $(\mathcal{L}, \diamond)$. This proves the theorem. ∎

Since groups and NAFIL loops are both invertible loops, then the coset product in Theorem 6 is not necessarily a NAFIL; it could also be a group. However, there are certain conditions under which the coset product is a NAFIL.

Corollary 1. *If $(E, *)$ and (C, Φ) are invertible loops, then $(\mathcal{L}, \diamond) = (E, *)X(C, \Phi)$ is a NAFIL if $(E, *)$ or any of the loops (C, ϕ_{pq}) under (C, Φ) is a NAFIL.*

This simply means that if at least one of the generating systems $(E, *)$ or (C, Φ) of $(\mathcal{L}, \diamond)$ is a NAFIL, then $(\mathcal{L}, \diamond)$ will also be a NAFIL. However, $(\mathcal{L}, \diamond)$ can also be a NAFIL even if its generating systems are all groups. This is the case if at least two of the groups (C, ϕ_{pq}) under (C, Φ) are not isomorphic.

In the previous theorems, we determined what kind of coset product results if its generating systems are given. The next theorem deals with the case when the coset product is given as a loop and we wish to determine what its generating systems are. Here we consider the case of a Type B loop.

Theorem 7. *If $(\mathcal{L}, \diamond) = (E, *)X(C, \Phi)$ is a coset product that is an invertible loop, then:*

(a) *$(E, *)$ is an invertible loop.*

(**b**) *The systems under (C, Φ) are such that:* (**b1**) *(C, ϕ_{pq}) is at least a quasi-group, where c_1 is at least a right identity if $q = 1$ and at least a left identity if $p = 1$; in particular, (C, ϕ_{11}) must be at least a loop and* (**b2**) *if $p, q \neq 1$, then (C, ϕ_{pq}) and (C, ϕ_{qp}) must be at least loops with c_1 as a common identity element such that either $\phi_{pq} = \phi_{qp}$, in which case the loops are invertible, or else every left (right) inverse of (C, ϕ_{pq}) is a right (left) inverse of (C, ϕ_{qp}).*

Proof. (**a**) Since $(\mathcal{L}, \diamond)$ is an invertible loop, then it satisfies A3. Let (e_1, c_1) be the identity and let (e_x, c_y) be any element of $\mathcal{L}$. Then, by A2 and Eq. (D5.1), it follows that

(T7.1)
$$(e_1, c_1) \diamond (e_x, c_y) = (e_1 * e_x, \, c_1 \phi_{1x} c_y) = (e_x, c_y)$$
$$(e_x, c_y) \diamond (e_1, c_1) = (e_x * e_1, \, c_y \phi_{x1} c_1) = (e_x, c_y)$$

which imply that

$$e_1 * e_x = e_x, \quad \text{and} \quad e_x * e_1 = e_x$$

Hence, $(E, *)$ has a unique identity element e_1 and is therefore a loop. Now, let (e_p, c_a) and (e_q, c_b) be inverses in $(\mathcal{L}, \diamond)$. Then, by A3 and Eq. (D5.1), it follows that

(T7.2)
$$(e_p, c_a) \diamond (e_q, c_b) = (e_p * e_q, \, c_a \phi_{pq} c_b) = (e_1, c_1)$$
$$(e_q, c_b) \diamond (e_p, c_a) = (e_q * e_p, \, c_b \phi_{qp} c_a) = (e_1, c_1)$$

which imply that:

$$e_p * e_q = e_1 \quad \text{and} \quad e_q * e_p = e_1$$

This means that e_p and e_q are inverses in $(E, *)$ and therefore it follows that the loop $(E, *)$ satisfies A3 and is at least an invertible loop.

(**b**) Let (e_1, c_1) be the identity of $(\mathcal{L}, \diamond)$. (**b1**) By Theorem 3, (C, ϕ_{pq}) is at least a quasigroup. Let $(e_x, c_y) \in \mathcal{L}$, where $x \neq 1$. By Eqs. (T7.1), we find that:

$$c_1 \phi_{1x} c_y = c_y \quad \text{and} \quad c_y \phi_{x1} c_1 = c_y$$

which imply that c_1 is at least a *left identity* in (C, ϕ_{1x}) and a *right identity* in (C, ϕ_{x1}). However, if $x = 1$, then c_1 is a unique identity and (C, ϕ_{11}) is at least a loop. (**b2**) Let (e_p, c_a) and (e_q, c_b) be inverses in $(\mathcal{L}, \diamond)$. Since $(\mathcal{L}, \diamond)$ satisfies *A3*, it follows from Eqs. (T7.2) that

$$c_a \phi_{pq} c_b = c_1 \quad \text{and} \quad c_b \phi_{qp} c_a = c_1$$

which implies that (C, ϕ_{pq}) and (C, ϕ_{qp}) are loops with a common identity element c_1 such that: either $\phi_{pq} = \phi_{qp}$, in which case c_a and c_b are inverses so that the loops are invertible, or else c_a is the *left inverse* of c_b in (C, ϕ_{pq}) and c_a is its *right inverse* in (C, ϕ_{qp}). This completes the proof of Theorem 7. ∎

In Theorem 4, we have shown that the system $(B, \times)$ is a quasigroup whose operation $\times$ is induced by the operation $*$ of $(E, *)$ on B. In Theorem 5, we found that if the generating systems $(E, *)$ and (C, Φ) of $(\mathcal{L}, \diamond)$ are loops and $B = \{B_1, \ldots, B_k\}$ is the E-partition of $\mathcal{L}$ $(mod \ B_1)$, then $(B_1, \diamond)$ is a normal subsystem of $(\mathcal{L}, \diamond)$ and

that $(B, \times)$ is a loop isomorphic to $(E, *)$. This indicates that there is a close connection between the structures of the systems $(\mathcal{L}, \diamond)$ and $(B, \times)$ which we shall now consider [6, 8].

Definition 10. *Let $(\mathcal{L}, \diamond)$ and $(B, \times)$ be two algebraic systems. A mapping $\theta : \mathcal{L} \to B$ is a **homomorphism** from $(\mathcal{L}, \diamond)$ to $(B, \times)$ if for any $\ell_a, \ell_b \in \mathcal{L}$ the following relation holds:*

$$\theta(\ell_a \diamond \ell_b) = \theta(\ell_a) \times \theta(\ell_b)$$

*In this case, $(B, \times)$ is called the **homomorphic image** of $(\mathcal{L}, \diamond)$. If the map θ is one-to-one and onto, the homomorphism is called an **isomorphism.***

This definition holds for two algebraic systems with a common axiom type. In the non-trivial case, the map $\theta : \mathcal{L} \to B$ is many-to-one. For groups, the homomorphism preserves several properties of $(\mathcal{L}, \diamond)$ which are carried on to $(B, \times)$. Thus, if $(\mathcal{L}, \diamond)$ is a group, then $(B, \times)$ is also a group. For non-associative loops in general, only the loop properties of $(\mathcal{L}, \diamond)$ are preserved. However, since the group is also an invertible loop, then a non-associative loop (like a NAFIL) can have a factor system that is a group. Accordingly, we call this a **loop homomorphism**. An isomorphism of an algebraic system (like a quasigroup or a loop) onto itself is called an **automorphism**. Moreover, $(B, \times)$ is also called the **kernel** of the homomorphism.

Theorem 8. *Let $(\mathcal{L}, \diamond) = (E, *) X (C, \Phi)$ be a coset product of order $n = km$ that is an invertible loop, where (C, Φ) is of Type A. Let $B = \{B_p \mid p = 1, ..., k\}$ (**E-partition**) and $D = \{D_q \mid q = 1, ..., m\}$ (**C-partition**) be partitions of $\mathcal{L}$ such that*

(T8.1) $B_p = \{(e_p, c_j) \in \mathcal{L} \mid j = 1, ..., m\}$

(T8.2) $D_q = \{(e_i, c_q) \in \mathcal{L} \mid i = 1, \ldots, k\}$

*If (e_1, c_1) is the identity of $(\mathcal{L}, \diamond)$, where e_1 is the identity of $(E, *)$ and c_1 is the common identity element of (C, Φ) for all $\phi_{ij} \in \Phi$, then: (**a**) $(B_1, \diamond)$ is a subsystem of $(\mathcal{L}, \diamond)$ and is isomorphic to (C, ϕ_{11}). (**b**) The system $(B, \times)$, where $\times$ is coset cell multiplication, is an invertible loop isomorphic to $(E, *)$. (**c**) If $D_1 = \{(e_i, c_1) \in \mathcal{L} \mid i = 1, ..., k\}$, then $(D_1, \diamond)$ is a subsystem of $(\mathcal{L}, \diamond)$. Moreover, $(D_1, \diamond)$ is isomorphic to $(E, *)$ and hence also to $(B, \times)$. (**d**) $(\mathcal{L}, \diamond)$ and $(B, \times)$ are homomorphic and $(B, \times)$ is a factor system of $(\mathcal{L}, \diamond)$. Hence, , $(B_1, \diamond)$ is normal.*

Proof. (**a**) By Eq. (T8.1), we have: $B_1 = \{(e_1, c_j) \in \mathcal{L} \mid j = 1, ..., m\}$. Hence, if (e_1, c_a) and (e_1, c_b) are any two elements of B_1, then their product is $(e_1, c_a) \diamond (e_1, c_b) = (e_1, c_a \phi_{11} c_b) \in B_1$, where $\phi_{11} \in \Phi$. Hence, $(B_1, \diamond)$ is a subsystem of $(\mathcal{L}, \diamond)$ and is therefore an invertible loop. We also find that the correspondence:

$$(e_1, c_a) \leftrightarrow c_a, \ (e_1, c_b) \leftrightarrow c_b, \quad (e_1, c_a) \diamond (e_1, c_b) \leftrightarrow c_a \phi_{11} c_b$$

defines an isomorphism between $(B_1, \diamond)$ and (C, ϕ_{11}).

(**b**) If $(e_p, c_a) \in B_p$ and $(e_q, c_b) \in B_q$, then $(e_p, c_a) \diamond (e_q, c_b) = (e_p * e_q, c_a \phi_{pq} c_b) = (e_r, c_a \phi_{pq} c_b) \in B_r$, where $e_r = e_p * e_q \in E$. Therefore, we can write $B_p \times B_q = B_r$ where

(T8.3) $B_p \times B_q = \{(e_p * e_q, c_a \phi_{pq} c_b) \mid a, b = 1, \ldots, m\}$

which implies that $(B, \times)$ is at least a groupoid. Moreover, the correspondence

$$B_p \leftrightarrow e_p, \ B_q \leftrightarrow e_q, \ B_p \times B_q \leftrightarrow e_p * e_q$$

defines an isomorphism between $(B, \times)$ and $(E, *)$. Since $(\mathcal{L}, \diamond)$ is an invertible loop, then by Theorem 7 so is $(E, *)$. Moreover, since $(B, \times)$ is isomorphic to $(E, *)$, then $(B, \times)$ is also an invertible loop.

(**c**) Let (e_p, c_1) and (e_q, c_1) be elements of D_1. Then we find that $(e_p, c_1) \diamond (e_q, c_1) = (e_p * e_q, c_1\phi_{pq}c_1) = (e_r, c_1) \in D_1$, where $e_r = e_p * e_q \in E$ and $c_1 = c_1\phi_{pq}c_1 \in C$ (since c_1 is a common identity for all $\phi_{pq} \in \Phi$). Thus, $(D_1, \diamond)$ is a subsystem of $(\mathcal{L}, \diamond)$. Clearly, the correspondence:

$$(e_p, c_1) \leftrightarrow e_p, \quad (e_q, c_1) \leftrightarrow e_q, \quad (e_p, c_1) \diamond (e_q, c_1) \leftrightarrow e_p * e_q$$

is an isomorphism between $(D_1, \diamond)$ and $(E, *)$ and therefore $(D_1, \diamond)$ is also an invertible loop like $(E, *)$. Since $(B, \times)$ is also isomorphic to $(E, *)$, then $(B, \times)$ and $(D_1, \diamond)$ are also isomorphic.

(**d**) By Definition 10, $(\mathcal{L}, \diamond)$ and $(B, \times)$ are homomorphic if the map $\theta : \mathcal{L} \to B$ satisfies the relation: $\theta[(e_i, c_u) \diamond (e_j, c_v)] = \theta(e_i, c_u) \times \theta(e_j, c_v)$ for all $(e_i, c_u), (e_j, c_v) \in \mathcal{L}$. This is clearly satisfied by $(\mathcal{L}, \diamond)$ and $(B, \times)$. To see this, let $\theta(e_i, c_u) \to B_i$ and let $\theta(e_j, c_v) \to B_j$. Then we find that

$$\theta(e_i, c_u) \times \theta(e_j, c_v) \to B_i \times B_j$$
$$\theta[(e_i, c_u) \diamond (e_j, c_v)] = \theta(e_i * e_j, c_u\phi_{ij}c_v) = \theta(e_k, c_w) \to B_k$$

where $e_k = e_i * e_j$ and $c_w = c_u\phi_{ij}c_v$. Hence, $(B, \times)$ is a *factor system* of $(\mathcal{L}, \diamond)$. This implies that $(B_1, \diamond)$ is normal. ∎

We have seen that $(\mathcal{L}, \diamond)$ and $(B, \times)$ are homomorphic and that $(B_1, \diamond)$ is a normal subsystem of $(\mathcal{L}, \diamond)$. Moreover, B_1 is the identity of $(B, \times)$. Thus $\theta(e_1, c_u) \to B_1$ means that the elements $(e_1, c_u) \in \mathcal{L}$ are mapped by θ onto the identity element B_1 of $(B, \times)$. Following the usual terminology, we shall call $(B_1, \diamond)$ the **kernel** of the homomorphism of $(\mathcal{L}, \diamond)$ into $(B, \times)$ and call $(\mathcal{L}, \diamond)$ a **factorable** system. We also note that $(E, *)$ is isomorphic to the subsystem $(D_1, \diamond)$. However, $(D_1, \diamond)$ is not necessarily normal and hence it does not necessarily form a factor system of $(\mathcal{L}, \diamond)$. This is because the system (C, Φ) is a multi-ϕ. If it happens that $(D_1, \diamond)$ is normal, then $(\mathcal{L}, \diamond)$ is called an **extension** of $(E, *)$. This will be the case when $(\mathcal{L}, \diamond)$ is a direct product where (C, Φ) is a mono-ϕ.

The cells D_q of the *C-partition* D defined in Theorem 8 do not form a factor system if at least two operations of Φ are not equal. By Definition 4, two binary operations ϕ_{pq} and ϕ_{rs} over the same set C are said to be *equal*, that is $\phi_{pq} = \phi_{rs}$, if and only if $c_i\phi_{pq}c_j = c_i\phi_{rs}c_j$ for all $c_i, c_j \in C$. This means that if $\phi_{pq} = \phi_{rs}$, then the systems (C, ϕ_{pq}) and (C, ϕ_{rs}) have identical Cayley tables and hence are isomorphic. Because of this, we shall call them *identically isomorphic* This distinction is important when dealing with quasigroup-type systems whose Cayley tables are Latin squares. Two identically isomorphic quasigroup-type systems have identical Cayley tables. If they are simply isomorphic, their Cayley tables are not necessarily identical but are equivalent (isotopic) Latin squares.

Theorem 8 is true even if $(\mathcal{L}, \diamond)$ is only a loop that is not invertible. However, if the systems under (C, Φ) do not have a common identity element (Type B), then $(D_1, \diamond)$ will not be a subsystem of $(\mathcal{L}, \diamond)$. In this case, $(\mathcal{L}, \diamond)$ will not have any subsystem isomorphic to $(B, \times)$ and hence to $(E, *)$. Thus, $(\mathcal{L}, \diamond)$ is not an extension of $(E, *)$.

Theorem 9. *Every loop* $(L, \star)$ *of order* $n = km$ *with a non-trivial normal subloop* $(\mathcal{B}_1, \star)$ *of order* m *is a coset product of the form* $(\mathcal{L}, \diamond) = (E, *)\mathsf{X}(C, \Phi),$ *where* $(E, *)$ *is a loop of order* k *and* (C, Φ) *is a multi-ϕ system of order* $m.$

Proof. To prove this theorem, it is sufficient to show that the loop $(L, \star)$ with the normal subsystem $(\mathcal{B}_1, \star)$ is isomorphic to a loop of the form $(\mathcal{L}, \diamond) = (E, *)\mathsf{X}(C, \Phi),$ where $(E, *)$ is a loop of order k, (C, Φ) is a multi-ϕ system of order m, and the operation $\diamond$ is defined by the composition rule (D5.1):

$$(e_p, c_a) \diamond (e_q, c_b) = (e_p * e_q, \ c_a \phi_{pq} c_b).$$

By Theorem 5 a coset product loop $(\mathcal{L}, \diamond) = (E, *)\mathsf{X}(C, \Phi)$ of order $n = km$ with a normal subloop $(B_1, \diamond)$ of order k can be constructed. We now claim that by a proper choice of generating systems $(E, *)$ and (C, Φ), it is always possible to construct such a loop $(\mathcal{L}, \diamond)$ that is isomorphic to the given loop $(L, \star)$.

By hypothesis, $(L, \star)$ has a normal subloop $(\mathcal{B}_1, \star)$ of order m. Hence, by Definition 6, the set $\mathcal{B} = \{\mathcal{B}_1, ..., \mathcal{B}_k\}$ of cosets of $\mathcal{B}_1$ forms a factor loop $(\mathcal{B}, \mathsf{X})$ of order k, where X is coset multiplication. For the loops $(L, \star)$ and $(\mathcal{L}, \diamond)$ to be isomorphic, they must satisfy the following necessary conditions: The coset product loop $(\mathcal{L}, \diamond)$ must be such that **(a)** its normal subloop $(B_1, \diamond)$ is isomorphic to $(\mathcal{B}_1, \star)$ and **(b)** its factor loop $(B, \times)$ is isomorphic to $(\mathcal{B}, \mathsf{X})$.

Let $L = \{\ell_1, ..., \ell_{km}\}$ and let $\mathcal{L} = \{(e_x, c_y) \mid e_x \in E, \ c_y \in C\}$, where $E = \{e_1, ..., e_k\}$ and $C = \{c_1, ..., c_m\}$. Next, let the elements of $\mathcal{L}$ be paired one-to-one with the elements of L by the rule:

(T9.1) $$(e_x, c_y) \leftrightarrow \ell_h$$

where $h = m(x - 1) + y$ for all $x = 1, ..., k$ and $y = 1, ..., m$. Partition the n elements of $\mathcal{L}$ into k cells $B_x = \{(e_x, c_y) \mid y = 1, ..., m\}$, where $x = 1, ..., k$, and let $B = \{B_1, ..., B_k\}$ represent this E-partition.

To satisfy condition (a), we now let $(B_1, \diamond) \cong (\mathcal{B}_1, \star)$ by means of the correspondence rule (T9.1) for $x = 1$ which becomes: $(e_1, c_y) \leftrightarrow \ell_y$. Now, if $(e_1, c_p), (e_1, c_q) \in B_1$, then $(e_1, c_p) \diamond (e_1, c_q) = (e_1 * e_1, \ c_p \phi_{11} c_q) = (e_1, c_r) \in B_1$, where $c_r = c_p \phi_{11} c_q$. By the correspondence rule, we have: $(e_1, c_p) \leftrightarrow \ell_p$ and $(e_1, c_q) \leftrightarrow \ell_q$. Hence, we must also have $(e_1, c_p) \diamond (e_1, c_q) \leftrightarrow \ell_p \star \ell_q$. If $\ell_p \star \ell_q = \ell_r$ in $(\mathcal{B}_1, \star)$, then we must set: $(e_1, c_r) \leftrightarrow \ell_r$. It can be shown that it is always possible to choose ϕ_{11} so that this correspondence is satisfied and is an isomorphism.

To satisfy condition (b) that $(B, \times)$ is isomorphic to $(\mathcal{B}, \mathsf{X})$, we simply set the correspondence: $B_i \leftrightarrow \mathcal{B}_i$ for all $i = 1, ..., k$. This is possible because $(B, \times)$ and $(\mathcal{B}, \mathsf{X})$ are loops of the same order k, where B_1 is the identity of B and $\mathcal{B}_1$ is the identity of $\mathcal{B}$. As in case (a), if $(e_i, c_p) \in B_i$ and $(e_j, c_q) \in B_j$, we can set the correspondence: $(e_i, c_p) \leftrightarrow \ell_{p'}$ and $(e_i, c_q) \leftrightarrow \ell_{q'}$, where $\ell_{p'} \in \mathcal{B}_i$ $(p' = m(i - 1) + p)$ and $\ell_{q'} \in \mathcal{B}_j$ $(q' = m(j - 1) + q)$. Since $(e_i, c_p) \diamond (e_j, c_q) = (e_i * e_j, \ c_p \phi_{ij} c_j)$, then, by this correspondence, we have:

(T9.2) $$(e_i, c_p) \leftrightarrow \ell_{p'}, \ (e_i, c_q) \leftrightarrow \ell_{q'}, \ \text{and} \ (e_i, c_p) \diamond (e_j, c_q) \leftrightarrow \ell_{p'} \star \ell_{q'}$$

Again, it is always possible to choose ϕ_{ij} so that this correspondence is satisfied. This shows that the isomorphic correspondence $B_i \leftrightarrow \mathcal{B}_i$ holds true in general for the operations $\diamond$ and $\star$ and that (T9.2) defines an isomorphism.

The above arguments (a) and (b) show that a loop $(L, \star)$ with a normal subloop $(\mathcal{B}_1, \star)$ is isomorphic to a coset product loop of the form $(\mathcal{L}, \diamond) = (E, *)\mathsf{X}(C, \Phi)$. This proves the theorem. ∎

This theorem also holds for any loop with a non-trivial subsystem of even order $n = 2m$. In the case of NAFIL loops, the systems $(B_1, \diamond)$, $(B, \times)$, and $(E, *)$ must also be invertible. It is important to note that the NAFIL and the group are both invertible loops (axiom type $A[1,4,2,3]$). This means that a NAFIL can have a group as a subsystem. It is therefore possible for a factor system $(B, \times)$ to be a group even if $(\mathcal{L}, \diamond)$ is a NAFIL. This is the case when $(E, *)$, which is isomorphic to $(B, \times)$, is a group.

Since a loop $(\mathcal{L}, \diamond)$ may have more than one non-trivial normal subsystem, then such a loop can be expressed as a coset product with respect to each of its normal subsystems. This is related to the various coset decompositions of a loop with respect to its normal subsystems: each decomposition determines a unique E-partition of $\mathcal{L}$.

Nucleus and Center of a Loop. In a loop like an invertible loop, there exist certain elements (like the identity) that associate with all elements of the loop. Such elements form special subsets called the **nuclei** and **center** of the loop [4, 5].

Definition 11. *The **left nucleus** of a loop $(\mathcal{L}, \diamond)$ is the set of all elements $a \in \mathcal{L}$ such that $a(xy) = (ax)y$ for all $x, y \in \mathcal{L}$. The **middle nucleus** and **right nucleus** are similarly defined. The intersection of these three nuclei is simply called the **nucleus** $\mathcal{N}(\mathcal{L})$ of the loop. The set of all elements in the nucleus which commute with all elements of the loop is called the **center** $Z(\mathcal{L})$ of the loop.*

Every nucleus is a subloop of the loop. It can be shown that the center is a normal subloop of the loop and thus forms the **kernel** of a loop homomorphism. Clearly, every loop has a nucleus and hence also a center. For instance, the identity element of a loop always forms a trivial center.

For a group G (which is associative), the center is simply $Z(G) = \{b \in G \mid ab = ba \text{ for all } a \in G\}$. Hence, the center $Z(G)$ is always an abelian subgroup. Moreover, it can be shown that $Z(G)$ is normal. For abelian groups, every normal subgroup thus qualifies as a center. Since an abelian group may have several normal subgroups, we shall only consider the intersection of all normal subgroups of an abelian group to be its **proper center**.

$\diamond$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	1	4	3	6	5
3	3	4	5	6	1	2
4	4	3	6	5	2	1
5	5	6	1	2	4	3
6	6	5	2	1	3	4

$\Longrightarrow$

$\times$	B_1	B_2	B_3
B_1	B_1	B_2	B_3
B_2	B_2	B_3	B_1
B_3	B_3	B_1	B_2

Table 4(A). NAFIL loop $(\mathcal{L}, \diamond)$

Table 4(B). Factor group $(B, \times) \cong C_3$

For NAFIL loops in general, $Z(\mathcal{L}) = \{b \in \mathcal{N}(\mathcal{L}) \mid ab = ba \text{ for all } a \in \mathcal{L}\}$, where $\mathcal{N}(\mathcal{L})$ is the nucleus of $(\mathcal{L}, \diamond)$. This means that every element of $Z(\mathcal{L})$ must associate with all elements of $\mathcal{L}$. Moreover, $Z(\mathcal{L})$ is always a normal subloop of $(\mathcal{L}, \diamond)$. For instance, the center of the abelian NAFIL $(\mathcal{L}, \diamond)$ shown above is $Z(\mathcal{L}) = \{1, 2\}$ which is a normal subgroup of $(\mathcal{L}, \diamond)$. It is easy to verify from the Cayley table that the elements of $Z(\mathcal{L})$ commute and associate with all elements of $\mathcal{L}$. Moreover,

we also see that the cosets $B_1 = \{1, 2\}$, $B_2 = \{3, 4\}$, $B_3 = \{5, 6\}$ of this center $Z(\mathcal{L}) \equiv B_1$ form a factor group $(B, \times)$ of order $m = 3$, where $B = \{B_1, B_2, B_3\}$, isomorphic to the cyclic group C_3. This also shows that $Z(\mathcal{L})$ is normal.

Theorem 10. *Every loop with a non-trivial center is a coset product.*

Proof. This follows easily from Theorem 9 since the center of a loop is always a normal subloop of the loop. ∎

This theorem holds for all loops like NAFIL loops and groups. Its importance lies in the fact that the center of a loop is a very special normal subloop. The unique decomposition of a loop in terms of the cosets of its center enables us to determine many aspects of its structure. For instance, the center $Z(\mathcal{L})$ of a loop $(\mathcal{L}, \diamond)$ always forms the kernel of a loop homomorphism [6, 8] by means of which it is possible to obtain an **upper** or **ascending central series** [6, 8]: $1 \subseteq Z_1 \subseteq Z_2 \subseteq Z_3 \subseteq ...$, where $Z_1 = Z(\mathcal{L})$ and Z_{i+1} is the full pre-image in $\mathcal{L}$ of $Z(\mathcal{L}/Z_i)$.

Other properties of coset products include:

Theorem 11. *The coset product* $(\mathcal{L}, \diamond) = (E, *)\mathsf{X}(C, \Phi)$ *is abelian if* $*$ *and every* $\phi_{pq} \in \Phi$ *are commutative.*

The proof of this theorem is trivial.

An important example of a coset product with Type B (C, Φ) loops is the **Octonion loop** $(\mathbb{O}_L, \star) = (E, *)\mathsf{X}(C, \Phi)$ of order 16 which is a NAFIL [3]. The center of this loop is the cyclic group C_2 of order 2 and its factor group is an abelian group of order 8 (isomorphic to the Klein group K_8). However, the octonion does not have any abelian subgroup of order 8.

2.1.5. **Direct Products.** The block product reduces to the *direct product* if Φ is a mono-ϕ. Although the direct product structure is primarily associated with groups and related associative systems, many quasigroups also have this structure. In particular, a direct product is always an extension of $(E, *)$ by (C, Φ). The following theorems will deal with some of the basic properties of direct products in general.

Theorem 12. *The direct product* $(\mathcal{L}, \diamond) = (E, *)\mathsf{X}(C, \Phi)$ *is a group if both* $(E, *)$ *and* (C, Φ) *are groups, and conversely. Otherwise, it is a NAFIL if* (C, Φ) *or* $(E, *)$*, or both are NAFIL loops.*

Theorem 13. *Let* $(\mathcal{L}, \diamond) = (E, *)\mathsf{X}(C, \Phi)$ *be a direct product of type A[1,4,2,3], where* $(E, *)$ *and* (C, Φ) *have proper subsystems* $(\overline{E}, *)$ *and* $(\overline{C}, \Phi)$*, respectively. Then* $(\mathcal{L}, \diamond)$ *has subsystems isomorphic to the following:* $(E, *)$, $(\overline{E}, *)$, (C, Φ), $(\overline{C}, \Phi)$, $(E, *)\mathsf{X}(\overline{C}, \Phi)$, $(\overline{E}, *)\mathsf{X}(C, \Phi)$, *and* $(\overline{E}, *)\mathsf{X}(\overline{C}, \Phi)$.

Any subsystem of $(\mathcal{L}, \diamond)$ that is isomorphic to either $(E, *)$ or (C, Φ) will be called an **isomorphic image** of $(E, *)$ or (C, Φ) in $(\mathcal{L}, \diamond)$.

Theorem 14. *Let* $(\mathcal{L}, \diamond) = (E, *)\mathsf{X}(C, \Phi)$ *be a direct product of type A[1,4,2,3] (invertible loop) and let* $(\overline{E}, \diamond)$ *and* $(\overline{C}, \diamond)$ *be the isomorphic images in* $(\mathcal{L}, \diamond)$ *of*

$(E, *)$ and (C, Φ), respectively, where

$$\overline{E} = \{(e_i, c_1) \in \mathcal{L} \mid i = 1, \ldots, k\}$$
$$\overline{C} = \{(e_1, c_j) \in \mathcal{L} \mid j = 1, \ldots, m\}$$

Then the set $D = \{D_q \mid q = 1, ..., m\}$ of cosets of $\overline{E}$ (**C-partition**) and the set $B = \{B_p \mid p = 1, ..., k\}$ of cosets of $\overline{C}$ (**E-partition**) form factor systems $(D, \times_D)$ and $(B, \times_B)$ isomorphic to (C, Φ) and $(B, \times)$, respectively, where $\times_B$ and $\times_D$ are operations of coset cell multiplication.

This theorem shows that the direct product $(\mathcal{L}, \diamond) = (E, *)\mathsf{X}(C, \Phi)$, which contains subsystems isomorphic to $(E, *)$ and (C, Φ), is an *extension* of $(E, *)$ by (C, Φ).

Theorem 15. *If $(E, *)$ and (C, Φ) are any two systems of type A[1,4,2,3], then the direct products $(E, *)\mathsf{X}(C, \Phi)$ and $(C, \Phi)\mathsf{X}(E, *)$ are isomorphic.*

The proofs of the above theorems are simple.

2.2. **Non-Lagrangian Systems.** One unique characteristic of certain NAFIL loops that distinguishes them from groups is that they are **non-Lagrangian**, that is, they have non-trivial subsystems whose orders are not divisors of the order of their underlying set. Thus, the smallest NAFIL $(L_5, *)$ of order $n = 5$ is non-Lagrangian because it has subsystems of order $m = 2$. In fact there are numerous families of non-Lagrangian NAFIL loops.

For convenience, a subsystem will be called a **non-divisor** if its order is not a divisor of the order of its parent system. Otherwise, it will be called a **divisor**.

In a non-Lagrangian NAFIL, the cosets of a non-divisor subsystem do not determine a unique partition of the underlying set as is the case with coset groups. Hence, such subsystems are not *normal*.

There are also NAFIL loops in which all non-trivial subsystems are non-divisors. We call such NAFIL loops **anti-Lagrangian**. Such a NAFIL has no non-trivial normal subsystem and is therefore simple.

$*$	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9
2	2	1	4	3	6	5	8	9	7
3	3	4	1	2	7	8	9	6	5
4	4	3	2	1	8	9	5	7	6
5	5	6	7	8	9	1	2	4	3
6	6	5	8	9	1	7	3	2	4
7	7	8	9	6	2	3	4	5	1
8	8	9	5	7	3	4	6	1	2
9	9	7	6	5	4	2	1	3	8

Table 5. Anti-Lagrangian NAFIL $(L_9, *)$ of order $n = 9$.

As an example, the NAFIL $(L_9, *)$ of order $n = 9$ is anti-Lagrangian because its five non-trivial subsystems are all non-divisors: one of order 4 and four of order 2. These subsystems are: $(\{1, 2, 3, 4\}, *)$, $(\{1, 2\}, *)$, $(\{1, 3\}, *)$, $(\{1, 4\}, *)$, and $(\{1, 8\}, *)$.

The property of being non-Lagrangian only requires that the NAFIL has at least one non-divisor subsystem. Thus, there are also non-Lagrangian NAFIL loops with

divisor subsystems. As an example, the non-Lagrangian PAP NAFIL $(L_{10}, \diamond)$ of order $n = 10$ has subsystems of order 4 (non-divisor) and of orders 5 and 2 (divisors).

$\diamond$	1	2	3	4	5	6	7	8	9	10
1	1	2	3	4	5	6	7	8	9	10
2	2	1	5	3	4	7	6	10	8	9
3	3	4	1	5	2	8	9	6	10	7
4	4	5	2	1	3	9	10	7	6	8
5	5	3	4	2	1	10	8	9	7	6
6	6	7	8	9	10	1	2	3	4	5
7	7	6	10	8	9	2	1	5	3	4
8	8	9	6	10	7	3	4	1	5	2
9	9	10	7	6	8	4	5	2	1	3
10	10	8	9	7	6	5	3	4	2	1

Table 6. Non-Lagrangian NAFIL $(L_{10}, \diamond)$ with divisor and non-divisor subsystems.

The NAFIL $(L_{10}, \diamond)$ is the direct product of a cyclic group $(E, *)$ of prime order 2 and a non-Lagrangian NAFIL (C, Φ) of order 5 which has 4 subsystems of order 2. Analysis shows that $(L_{10}, \diamond)$ has the following subsystems: $(\{1,2,6,7\}, \diamond)$ which is of order 4 (non-divisor), as well as $(\{1,2,3,4,5\}, \diamond)$ of order 5 and $(\{1,6\}, \diamond)$ of order 2 (divisors). This is a special case of the following:

Theorem 16. *The direct product of a non-composite NAFIL (or group) of prime order and a non-Lagrangian NAFIL is a non-Lagrangian NAFIL.*

Proof. Let $(\mathcal{L}, \diamond) = (E, *) \mathsf{X} (C, \Phi)$ be a direct product of two invertible loops, where $(E, *)$ is non-composite of prime order k and (C, Φ) is non-Lagrangian of order m. To prove that $(\mathcal{L}, \diamond)$ is non-Lagrangian, we must show that it contains at least one subsystem $(\overline{\mathcal{L}}, \diamond)$ that is a non-divisor. By Definition 5 and Theorem 12, $(\mathcal{L}, \diamond)$ is a NAFIL of order $n = km$. Now let $(\overline{E}, *)$ be a non-trivial subsystem of order k' of $(E, *)$ and let $(\overline{C}, \Phi)$ be a non-divisor subsystem of order m' of (C, Φ). By Theorem 13, $(\mathcal{L}, \diamond)$ has subsystems isomorphic to $(\overline{E}, *)$ and $(\overline{C}, \Phi)$, respectively, and also to $(\overline{E}, *) \mathsf{X} (\overline{C}, \Phi)$ which is a subsystem of order $\mu = k'm'$. Next, let $(\overline{\mathcal{L}}, \diamond)$ be the subsystem isomorphic to $(\overline{E}, *) \mathsf{X} (\overline{C}, \Phi)$. Then $(\overline{\mathcal{L}}, \diamond)$ is a divisor of $(\mathcal{L}, \diamond)$ if and only if μ divides n, that is, if $\frac{n}{\mu} = $ integer. But $n = km$ and $\mu = k'm'$ so that

$$\frac{n}{\mu} = \frac{km}{k'm'} = \left(\frac{k}{k'}\right)\left(\frac{m}{m'}\right)$$

Because $(E, *)$ is non-composite of prime order k, then its only non-trivial subsystem $(\overline{E}, *) \cong (E, *)$ so that $k' = k$, $\left(\frac{k}{k'}\right) = 1$, and $\frac{n}{\mu} = \frac{m}{m'}$. Since, by hypothesis, $(\overline{C}, \Phi)$ is a non-divisor of (C, Φ), then its order m' is not a divisor of m and hence $\frac{n}{\mu} = \frac{m}{m'} \neq$ integer. This means that μ does not divide n which implies that $(\mathcal{L}, \diamond)$ contains a non-divisor subsystem $(\overline{\mathcal{L}}, \diamond) \cong (\overline{E}, *) \mathsf{X} (\overline{C}, \Phi)$. Therefore, $(\mathcal{L}, \diamond)$ is non-Lagrangian. Following the same argument as above, we can also show that $(\mathcal{L}, \diamond) = (E, *) \mathsf{X} (C, \Phi)$ is non-Lagrangian if (C, Φ) is non-composite of prime order and $(E, *)$ is non-Lagrangian. This completes the proof of this Theorem. ∎

Another example of this Theorem is the direct product of the composite NAFIL $(L_5, *)$ of prime order 5 and the cyclic group C_3 of order 3. This direct product is a

NAFIL of order $n = 15$ with non-trivial subsystems of orders 2 and 6 (non-divisors) and 3 and 5 (divisors).

Corollary 2. *The direct product of two composite NAFIL loops of prime order is non-Lagrangian.*

Proof. Let $(\mathcal{L}, \diamond) = (E, *)\mathsf{X}(C, \Phi)$ be a direct product of two composite invertible loops, where $(E, *)$ is of prime order k and (C, Φ) is of prime order m. Hence, $(\mathcal{L}, \diamond)$ is an invertible loop of order $n = km$. Now let $(\overline{E}, *)$ of order k' and $(\overline{C}, \Phi)$ of order m' be non-trivial subsystems of $(E, *)$ and (C, Φ), respectively. By Theorem 14, $(\mathcal{L}, \diamond)$ has a subsystem $(\overline{\mathcal{L}}, \diamond) \cong (\overline{E}, *)\mathsf{X}(\overline{C}, \Phi)$ which is of order $\mu = k'm'$. Then $(\overline{\mathcal{L}}, \diamond)$ is a divisor of $(\mathcal{L}, \diamond)$ if and only if μ divides n, that is, if $\frac{n}{\mu} = $ integer. But $n = km$ and $\mu = k'm'$ so that $\frac{n}{\mu} = \frac{km}{k'm'}$. Since k and m are prime, then μ divides m if and only if $k' = m$ and $m' = k$, that is, if $\mu = n$, in which case $(\overline{\mathcal{L}}, \diamond) \cong (\mathcal{L}, \diamond)$. For if $k' = m$ and $m' \neq k$, then $\frac{n}{\mu} = \frac{m}{k'} \neq $ integer since m is prime. Similarly, if $m' = k$ and $k' \neq m$, then $\frac{n}{\mu} = \frac{k}{m'} \neq $ integer. In both cases, we find that μ does not divide n. This means that $(\mathcal{L}, \diamond)$ contains at least one non-divisor subsystem $(\overline{\mathcal{L}}, \diamond)$ and is therefore non-Lagrangian. ∎

The simplest example of a NAFIL satisfying this Corollary is the direct product of the composite NAFIL $(L_5, *)$ of prime order 5 by itself. This is a NAFIL of order $n = 25$ with non-trivial subsystems of orders 2, 4, and 10 (non-divisors) and of order 5 (divisor).

In finite group theory, a group is called *simple* if it has no proper non-trivial normal subgroups. For instance, any group of prime order is simple because it has no non-trivial subgroup of any kind. This idea of a system being simple can also be extended to NAFIL loops.

Definition 12. *An invertible loop is called **simple** if it has no proper non-trivial normal subsystem. If it has no non-trivial subsystem of any kind, it is called **non-composite** or **plain** [10].*

In general, any invertible loop of prime order is simple. For instance, the smallest NAFIL loop $(L_5, *)$ of prime order 5 is simple. Most NAFIL loops of prime order $n \geq 7$ are simple and plain. Thus, of the 2,317 non-isomorphic abelian NAFIL loops of order 7, exactly 638 are plain [2].

∘	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7
2	2	3	1	5	6	7	4
3	3	1	2	7	4	5	6
4	4	5	6	1	7	3	2
5	5	6	7	2	1	4	3
6	6	7	4	3	2	1	5
7	7	4	5	6	3	2	1

Table 7(A). $(L_7, *$*Composite

⋆	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7
2	2	3	1	5	4	7	6
3	3	1	4	6	7	2	5
4	4	5	6	7	2	1	3
5	5	4	7	2	6	3	1
6	6	7	2	1	3	5	4
7	7	6	5	3	1	4	2

Table 7(B). Non-composite

Tables 7 show the Cayley tables of two simple NAFIL loops of order $n = 7$. 7(A) is the Cayley table of a simple NAFIL that is composite; it has non-trivial

subsystems of orders $m = 2, 3$ all of which are groups. On the other hand, 7(B) shows that of a simple NAFIL that is non-composite (*plain*).

The identification and study of simple NAFIL loops is very important to the understanding of NAFIL structure. As in finite group theory where simple groups are known to be the building blocks of composite groups, simple NAFIL loops also play a similar role. Therefore, the classification of simple NAFIL loops is a central problem of NAFIL theory.

Remark 2. An invertible loop of even order $n = 2m$ is **not simple** if it contains at least one subsystem of order m. This is true for loops in general and it follows easily from the fact that a subsystem of order $m = n/2$ is always normal.

3. Non-Composite NAFIL Loops

The study of non-composite NAFIL loops has so far not been given much attention by loop theorists. Very little is known about these loops called **plain** [7] which, in some ways, are analogous to groups of prime order. Therefore, the identification and characterization of plain NAFIL loops is an important problem of NAFIL theory.

3.1. **Plain NAFIL Loops.** As in the case of prime order groups, the simplest kind of simple NAFIL is one that is not-composite: it has no non-trivial subsystems of any kind. There are many examples of this type of simple NAFIL called **plain** to distinguish them from those that are simple but composite. Such a system is also called **anti-associative** because it contains no non-trivial groups and hence A6 is not satisfied in any non-trivial way within it.

Plain NAFIL loops are analogous to groups of prime order and therefore they play an important role in the study of NAFIL structure. Studies have so far shown that all NAFIL loops of order $n = 5$ and 6 are composite and that there exists a number of plain NAFIL loops of order $n = 7$ one of which is shown in Table 7(B). Thus, the smallest plain NAFIL is of order $n = 7$. All plain NAFIL loops are of odd order and are anti-associative.

Like the groups of prime order which constitute a family of plain groups, there are also known families of plain NAFIL loops. One such family [7] consists of abelian NAFIL loops of odd order $n = 2m + 1$, where $m \geq 3$.

*	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7
2	2	3	4	5	6	7	1
3	3	4	2	6	7	1	5
4	4	6	5	7	1	3	2
5	5	6	7	1	4	2	3
6	6	7	1	2	3	5	4
7	7	1	5	3	2	4	6

PLAIN 7N

$$\xleftarrow{\quad transpose \quad}\rightarrow$$

*'	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7
2	2	3	4	5	6	7	1
3	3	4	2	6	7	1	5
4	4	5	6	7	1	2	3
5	5	6	7	1	4	3	2
6	6	7	1	3	2	5	4
7	7	1	5	2	3	4	6

PLAIN 7N-T

Table 8. Cayley tables of two plain NAFIL loops of order $n = 7$.

Remark 3. *So far, we have discussed some of the basic properties of composite and non-composite NAFIL loops. The important question is: How do we construct and analyze a particular loop? In our studies, we made use of a powerful computer*

software called **FINITAS** *[4]. This software was developed by a team of PUP researchers and students at the PUP SciTech R&D Center with the support of the Department of Science & Technology.*

References

[1] G. Birkhoff and S. MacLane, *A Survey of Modern Algebra*, Macmilland Company, New York (1958)

[2] R. E. Cawagas, *Determination and Characterization of NAFIL Loops of Small Order 5, 6, 7*, PUP Journal of Research & Exposition, Vol. 3, No. 1 (2004).

[3] ——, *Finite Invertible Loops of the Coset Product Type*, PUP Journal of Research & Exposition (2002), Vol. 2, Issue 1, pp. 11-20.

[4] ——, *FINITAS – A Software for the Construction and Analysis of Finite Algebraic Structures*, PUP Journal of Research and Exposition, Vol. 1, No. 1 , pp. 1-10 (1997). [See also: R. E. Cawagas, *AXIOMS - Software for the Construction and Analysis of Finite Quasigroups, Semigroups and Related Structures,* Proceedings of the Second Asian Mathematical Conference 1995, World Scientific, Singapore-New Jersey-London-Hong Kong (1998), 401 405.]

[5] ——, *Introduction to Non-Associative Finite Invertible Loops*, PUP Journal of Science & Technology, Vol. 1, No. 2 (2007)

[6] O. Chein, et al (Editors) *Quasigroups and Loops: Theory and Applications*, Sigma Series in Pure Mathematics, Helderman Verlag Berlin (1990).

[7] H. Griffin, *The abelian Quasi-Group*, American Journal of Mathematics, Vol. 62, Issue 1/4 (1940), pp. 725-737.

[8] H. O. Pflugfelder, *Quasigroups and Loops: Introduction*, Sigma Series in Pure Mathematics, Helderman Verlag Berlin (1990).

[9] D. J. S. Robinson, *A Course in the Theory of Groups*, Springer Verlag, New York (1982) [See also: B. Baumslag and B. Chandler, *Group Theory*, Schaum's Outline Series in Mathematics, McGraw-Hill Book Company (19680]

[10] J. D. H. Smith, *Mal'cev Varieties*, Lecture Notes in Mathematics 554, Springer-Verlag, Berlin·Heidelberg·New York (1976), pp. 96-112..

Raoul E. Cawagas, SciTech R&D Center, Polytechnic University of the Philippines, Sta. Mesa, Manila

E-mail address: raoulec1@yahoo.com